Amendments To The Claims

The listing of claims presented below will replace all prior versions, and listings, of claims in the application.

Listing of claims:

1. (**Currently Amended**) A method for realizing ~~**data security storage and algorithm**~~ **algorithms** storage by means of a removable semiconductor memory device, wherein the semiconductor memory device comprises a controller module as well as a universal interface module and a semiconductor storage medium module electrically connected with the controller module, respectively, ~~**wherein the semiconductor storage medium module comprises one or more semiconductor chips,**~~ characterized in that the method comprises the steps of:

dividing the semiconductor storage medium module into at least two logic memory spaces;

using at least one of the logic memory spaces for storing ~~**data to be protected, wherein data to be protected comprises an algorithm**~~ **algorithms, wherein the algorithms comprise self-defined algorithms**;

~~**setting up and storing a password for the semiconductor memory device and said at least one logic memory space;**~~

~~**certifying the password before read/write operation;**~~

~~**when writing the data to be protected in the semiconductor memory device, the controller module receiving the data from the universal interface and, after encrypting the data, storing the encrypted data in the semiconductor storage medium module; and**~~

~~when reading the data to be protected from the semiconductor memory device, the controller module decrypting the data and transmitting the decrypted data via the universal interface;~~

~~when executing an algorithm stored in the semiconductor storage medium module, the controller module receiving an algorithm invoking parameter from the universal interface, decrypting the algorithm corresponding to the algorithm invoking parameter, executing the decrypted algorithm, and transmitting a result of the execution via the universal interface~~ when realizing legal software protection through the algorithms, the method further comprises:

1) sending the algorithm involking instruction by a host in which a legal software is stored to a driver program of the semiconductor memory device through an API function invocation in the legal software, wherein the algorithm invoking instruction is then transmitted from the driver program to the controller module via the universal interface;

2) loading and running codes of an algorithm corresponding to a parameter of the algorithm invoking instruction to a designated address in the semiconductor memory device by the controller module, wherein a notice of algorithm invoking operation success is then returned to the driver program through the universal interface;

3) returning the notice to the API function invocation from the driver program;

4) when the legal software receives the notice, transmitting an inquiry command to the semiconductor memory device, and the semiconductor memory

device returning a reply result created by the algorithm; and

5) the legal software being corresponding state according to the returned reply result.

2. (canceled)

3. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ **algorithms** storage by means of a semiconductor memory device of claim 1, characterized in that the semiconductor storage medium module comprises a storage medium, or a combination of at least two storage media.

4. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ **algorithms** storage by means of a semiconductor memory device of claim 1, characterized in that the semiconductor memory device and said at least one logic memory space set up at least two levels of users passwords.

5. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ **algorithms** storage by means of a semiconductor memory device of claim 4, characterized in that certification of user passwords is implemented before operation in all logic memory spaces, or before operation in the logic memory spaces storing the ~~**data to be protected**~~ **algorithms**.

6. **(currently amended)** The method for realizing ~~**data security storage and**~~

~~algorithm~~ algorithms storage by means of a semiconductor memory device of claim 1, 4 or 5, characterized by setting up a database, and conducting access and authority management to the ~~data to be protected~~ algorithms by way of the database.

7. **(currently amended)** The method for realizing ~~data security storage and algorithm~~ algorithms storage by means of a semiconductor memory device of claim [[6]] 1, characterized in that ~~the authority comprises reading authority, writing authority, modifying authority, deleting authority and executing authority, each authority having the meaning of:~~

~~Reading authority: only allowing reading record data in the database;~~

~~Writing authority: only allowing writing new data in the database, but not covering the record data with the same record title;~~

~~Modifying authority: only allowing writing data in the database and covering the record data with the same record title;~~

~~Deleting authority: allowing deleting the database or records therein;~~

~~Executing authority: allowing executing record codes in the database, which is an authority with respect to a self-defined algorithm or function code and it is invalid to designate an executing authority for normal record data~~ after the step 1), the process of realizing legal software protection further comprises:

the semiconductor memory device certifying whether the parameter of the algorithm invoking instruction has been falsified, and if so, quitting the algorithm invoking operation.

8. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ algorithms storage by means of a semiconductor memory device of claim 1, characterized in that ~~**at least one of the logic memory spaces is used for storing data that does not need protection**~~ **after the step 1), the process of realizing legal software protection further comprises:**

the semiconductor memory device certifying an access authority of a user, and if the user does not have the access authority for algorithm, returning an authority error code.

9. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ algorithms storage by means of a semiconductor memory device of claim 1, characterized in that an anti-falsifying identification is performed to identify whether the ~~**transmitted or**~~ stored **[[data]]** algorithms is falsified or not.

10. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ algorithms algorithm storage by means of a semiconductor memory device of claim 9, characterized in that ~~**during transmitting or storing data, the anti-falsifying identification comprises the steps of:**~~

~~**A. invoking an encrypting algorithm to convert original data to obtain a conversion value X;**~~

~~**B. packing the original data and the conversion value X according to certain a format to form a data package;**~~

~~**C. transmitting or storing the data package; and**~~

~~during receiving or reading data, the anti-falsifying identification method comprises the steps of:~~

~~A. unpacking the data package according to the format to obtain the unpacked original data and the conversion value X;~~

~~B. invoking the encrypting algorithm to calculate a conversion value of the unpacked original data to obtain a conversion value Y;~~

~~C. comparing the calculated conversion value Y and the conversion value X to see whether they are equal to each other;~~

~~D. if the compared result is that Y and X are equal, indicating the data that have has not been falsified, and otherwise indicating that the data has been falsified~~ after the step 1), the process of realizing legal software protection further comprises:

the semiconductor memory device decrypting the algorithm, and if a process of decrypting and reading is not success, returning an algorithm error code.

11. **(currently amended)** The method for realizing ~~data security storage and algorithm~~ algorithms storage by means of a semiconductor memory device of claim 1 **[[or 9]]**, characterized ~~by using randomly changeable session key to encrypt the data during the data transmission~~ in that the algorithm invoking operation is circulated continuously at random interval, and if the semiconductor memory device fails to be detected, the algorithm is not invoked and the legal software quits.

12. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ **algorithms** storage by means of a semiconductor memory device of claim **[[11]]** 7, characterized in that ~~**the step of using randomly changeable session key to encrypt data comprises the steps of:**~~

~~**A. at the beginning of the data transmission, transmission end transmitting a request of exchanging session key and introducing at least one random number;**~~

~~**B. after receiving the exchanging session key request, the semiconductor memory device randomly creating at least one random number, converting the received random number and the created random number by a key generating algorithm to produce a session key, and then returning the random number created by the semiconductor memory device to the transmission end;**~~

~~**C. after the transmission end receives the returned random number, converting the returned random number and the random number introduced by the transmission end itself with the key generating algorithm to produce the session key**~~ **the algorithm invoking operation is circulated continuously at random interval, and if the semiconductor memory device fails to be detected, the algorithm is not involked and the legal software quits**.

13. **(currently amended)** The method for realizing ~~**data security storage and algorithm**~~ **algorithms** storage by means of a semiconductor memory device of claim **[[1]]** 8, characterized in that ~~**the data to be protected include documents, passwords, cipher keys, account numbers, digital certificates, encrypting**~~

~~algorithm, self defined algorithm, user information and user self-defined data~~ the algorithm invoking operation is circulated continuously at random interval, and if the semiconductor memory device fails to be detected, the algorithm is not invoked and the legal software quits.

14 - 21. (canceled)

22. (new) The method for realizing algorithms storage by means of a semiconductor memory device of claim 10, characterized in that the algorithm invoking operation is circulated continuously at random interval, and if the semiconductor memory device fails to be detected the algorithm is not invoked and the legal software quits.